APPENDIX A

Corporate Security Policy Series
Policy 11-01 - Camera Surveillance and Sharing of Surveillance Images and Data

Effective Date: June 17, 2011

Camera Surveillance and Sharing of Surveillance Images and Data

Introduction. Massport operates surveillance cameras to detect, observe and record situations that may pose, constitute, or result in a security risk, or a threat to life, property, or public safety within the confines of its property. Cameras are also used to aid in the management of our facilities and roadways through increased situational awareness.

Purpose. To establish guidelines for the proper use and sharing of video surveillance technologies within Massport.

Applicability. This policy applies to all Massport employees and other stakeholders who are given access to surveillance images or other output (e.g. data or metadata) from Massport surveillance sensors. If the persons or organizations are receiving images, data or metadata under a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU), the provisions of the MOA or MOU apply but shall at minimum include the provisions of this policy. In such cases this policy also applies to the parties to such MOA or MOU.

Scope. This policy covers all images, data, and metadata from video surveillance of Massport facilities by Massport owned or operated cameras or other surveillance sensors. This policy extends to verbal or written descriptions of surveillance imagery or data. Where Massport has entered into an agreement to share surveillance imagery and data with other organizations, said MOA or MOU will include the provisions of this policy. This policy does not extend to the video surveillance cameras of Massport tenants where there is no MOA/MOU governing their use or products.

Policy Provisions.

Failure to comply with the provisions of this policy may result in disciplinary action up to and including termination.

Access

Before Massport shares its camera images with third parties, either in real-time, near real time, or archival access, we will ensure the third parties understand and agree to comply with this policy. In the reverse situation, whenever we are using third party images, we will use the most restrictive use policies and procedures between Massport and the third party source of the images.

Real-time monitoring. Only the Director of Corporate Security may grant real-time monitoring access. People who wish to have real-time access to surveillance imagery or data or control of Pan-Tilt-Zoom (PTZ) cameras via computer link will apply to the Director of Corporate Security on the form provided in Massport Public Folders. Access can be granted to individuals or entire departments based on the request of the department heads making the request, and upon the justification provided.

Near-real-time viewing. Near real-time means the viewing is done within minutes and not more than 2 hours after the fact. It enable us to quickly see what happened when there is a situation that is ongoing but which began before anyone began to monitor it. A common example is a suspected terminal breach or a door alarm. Quick resolution by watching what happened shortly after it happened is extremely helpful in determining what actions to take to mitigate any unresolved, possibly ongoing threat situation.

Post event, archival access. We expect camera imagery from Massport cameras performing surveillance on Massport properties, to be viewed for legitimate purposes by approved Massport personnel, as well as others with legitimate need as determined, upon request, by the Director of Corporate Security. Examples would include the TSA, State Police, MassDOT, and various federal partners with responsibilities extending to our airports or seaports or other properties. We also expect to receive numerous requests by the press, private citizens, litigants and their counsel, etc. through the established FOIA process

Proper Uses

1. Routine uses are, but not necessarily limited to, facility situation awareness, forensic review of security or law enforcement violations and for use in administrative, civil, and criminal proceedings.
2. At no time will surveillance cameras or the images or other data they produce be used for other than official Massport-sanctioned operational, safety, security or law enforcement purposes. This means that no cameras will be used for viewing people of personal interest, idle amusement, or other unsanctioned purposes. Such archived records that are produced are the property of Massport and may additionally be protected under TSA guidelines as Sensitive Security Information (SSI).
3. No personal use may be made of any of these records, nor may they be removed from the archives for any reason without express permission by management and then only for authorized purposes consistent with TSA guidelines and official Massport requirements.
4. Display monitors may not be photographed using privately owned cell phone or smart phone cameras or regular digital or film cameras.
5. No images from Massport surveillance cameras may be put on You Tube or any other Internet host be it social media or web site, etc.
6. Only the Massport Communications Department may approve and post such imagery after consultation with the Director of Corporate Security.
7. At no time will a Massport surveillance camera to be used to make or allow observations or record images off Massport property, either inside a building or outside, with exceptions noted in Paragraph 7 below. To the extent practicable and feasible Massport will limit the field of view or display parameters of its imaging equipment so as to prevent unauthorized or accidental viewing beyond Massport Property boundaries. Manual override of these "image blocks" will be limited to senior members of the Massport security team in pursuit of exceptional cases as provided in the next paragraph.

8. *Exceptional cases*: While Massport surveillance cameras have been installed to focus on Massport property, images from Massport cameras may be provided to an authorized law enforcement agency for legitimate law enforcement purposes but only to the extent such access is consistent with applicable laws. For example, a camera that allows us to monitor Bremen Street Park might also provide incidental coverage of adjacent locations in East Boston. Upon request by such law enforcement agencies as the Boston Police, the State Police, or the FBI, the Authority may, at the discretion of the Authority, review its stored image database to identify images that may have probative value to a criminal investigation. We could also allow live monitoring if the situation warranted. The Authority will exercise its discretion on a case-by-case basis acting through and based upon judgment of the Authority's Electronic Imaging Use Review Committee. This committee consists of the Director of Corporate Security and Deputy Director of Corporate Security, Associate Chief Legal Counsel for Security or Assistant, and the Director of Information Technology. When specific issues relative to an operational department or a support department are involved in making this determination the relevant department heads will be invited to join the group to assist in making the proper determination.

Retention Period

9. The standard retention goal for surveillance imagery and associated data within Massport is 30 calendar days. Whenever images or data are deemed to have value beyond the 30-day retention period this information will be saved for those purposes until it is no longer needed. If there is any likelihood the images or data might be used in any form of civil or criminal litigation this it will be saved to a non re-writable DVD disc and maintained in a sealed envelope in a secure file cabinet with documented chain of custody. A virtual copy will also be placed in a special, limited access file extension as backup.

10. Surveillance camera images of known or suspected security incidents will be stored permanently or until a decision to erase (or remove overwrite protection) is made by the Director of Corporate Security in consultation with legal counsel and the appropriate staffs in the impacted departments. In conjunction with Massport data storage backup procedures, camera surveillance storage will be backed-up to an off-site location every 24 hours. Surveillance images are not considered Public Records under the provisions of Massachusetts General Laws.

Protected Information

11. All images must be reviewed by competent authority to determine the level of protection they must receive by virtue of their content. Competent authority in this instance is defined as the Director or Deputy Director of Corporate Security, the Security and Deputy Director of Aviation and Maritime Security, Massport Legal Counsel to Aviation and Maritime, Massport Legal Counsel for FOIA, or Chief Legal Counsel.

12. Presumption is made that any image of or data from a non-public area of a regulated airport or seaport facility is presumed to be either SSI or some other category of Protected Information which require competent review and possible redaction before release. When we are not comfortable making decisions on redaction we will refer the matter of imagery release of presumed SSI to the TSA.
13. Images of or data from public areas may also contain SSI or protected information but there is no presumption of SSI or other Protected Information (PI) content. There is always the presumption that all images for release must be reviewed by competent authority to ensure there is no PI involved.
14. Only the Secretary of Transportation or the TSA Administrator may release SSI information to persons with no inherent need-to-know.
15. The Director of Corporate Security in coordination with Legal Counsel and if need be the TSA BOS Counsel, may redact SSI information in order to release it to someone with no inherent need to know, provided the FOIA process has been followed or it is in response to a subpoena or request from a federal, state or local partner who has signed an MOU with Massport for imagery access.

Imagery and Data Security

16. From the instant of capture to its eventual storage or deletion, all images and associated data or metadata shall be afforded protection from unauthorized disclosure.
17. Images in soft and hard copy will be provided security in accordance with Massport Policy HR 8.14 Protected Information. Briefly this means that all reasonable means to prevent unauthorized disclosure shall be taken.
18. This includes preventing unauthorized viewing of camera monitors in the possession of those who have been given access to Massport images or data. This also includes any print from any surveillance image, or any verbal description of an image or set of images.
19. The intent is for Massport to review and approve or restrict information access consistent with all applicable laws, regulations, and rules that govern access to Massport-held information.
20. Care must be taken to prevent unauthorized access to files to prevent erasure or changes that would render those images suspect or inadmissible in any of the above administrative, civil, or criminal procedures.
21. The IT Department, in conjunction with the operational users of these camera surveillance systems will establish such protocols as are deemed necessary to limit the number of people with access to those files to those who are approved by the Director of Corporate Security. They shall cause audit logs of such file access to be created and maintained for at least six years, and to ensure that the permissions protocols for access, including but not limited to User ID and Password, tokens, firewalls, rules, constitute reasonable measures to prevent unauthorized disclosure. Care must also be taken to provide sufficient physical protection for the surveillance camera application and file servers and backup servers.

DEPARTMENT OF HOMELAND SECURITY
Transportation Security Administration

FOIA REQUEST CERTIFICATION

INSTRUCTIONS: FOIA Points-of-Contact (POCs) will complete Section II and forward responsive records by mail to the TSA Headquarters FOIA Office, TSA-20, or by e-mail to the tasking individual, unless otherwise noted and explained below. If the search identifies TSA has a large volume of responsive records, FOIA POCs must contact the FOIA Office as soon as possible following receipt of this issued form to provide a cost estimate prior to continuing to process the request. Questions should be directed to the FOIA Office at (571) 227-2300 or 866-FOIA-TSA (866-364-2872).

SECTION I. Case Suspense and Identification *(FOIA Office USE ONLY)*

Response Required On/Before:	Direct E-mail Replies to: TSA.FOIAPOCResponses@tsa.dhs.gov
FOIA Case No.: 2013 TSFO 01096	Date: 1/2/14

Action Office(s): FSD/BOS THOMAS BRADY, FSD/LGA HAYWOOD SLIFKIN, FSD/ORD MICHAEL PRESTLER/EDITH BIANCHI

Request Received From: Mr. Sai

Requester Seeks: *(see attached request for further description)*

SECTION II. FOIA POC

Part A. Contact Information

Name: Roger Blais Title: Program Analyst Phone No.: 617-620-4135

Part B. Recommendations *(check all that apply and provide appropriate responses)*

☒ 1. Release all responsive records. *(identify records and from where retrieved)*
The requestor is requesting the contract or agreement with other agencies regarding surveillance,or maintenance of surveil footage at Logan Airport. The requested information was negotiated by TSA HQs and Massport. Attached for your informa are the names of the points of contact. Recommend that information pertaining to Massport be coordinated with TSA HQs prior to release

☐ 2. Withhold select responsive records. *(explain)*

☐ 3. Withhold all responsive records. *(explain)*

☐ 4. No responsive records. Search failed to identify and/or locate responsive records. *(explain)*

☐ 5. Recommend FOIA Office contact the following DHS Component, TSA Office, and/or individuals identified in order to search for responsive records. *(identify)*

Part C. Cost Estimate

Search Time (hrs.) / Pay Band	Processing Time (hrs.) / Pay Band	Attorney Time (hrs.) / Pay Band
1.0 / I	1.0 / J	/
/	/	/
/	/	/

Part D. Response Certification

I certify that a search reasonably calculated to uncover all responsive records, paper and electronic, has been conducted and all responsive records have been reviewed, copied and provided to the HQ FOIA Office, TSA-20, or otherwise noted with explanations and/or recommendations provided herein.

FOIA POC Signature: Thomas C Brady PR Date: 1/5/2014

Previous editions of this form are obsolete.

Brady, Thomas C (TSA)

From: Blais, Roger
Sent: Thursday, January 02, 2014 11:28 AM
To: Brady, Thomas C (TSA)
Subject: RE: 2013-TSFO-01096
Attachments: MOA TSA CCCS_8 17 11.docx; MOD P00002 HSTS04-09-H-CT7015, Fully Executed.pdf; ASP BOS 09HCT7015 ER1 060612.pdf; HSTS04-09-H-CT7015_P00001_POP Extension.doc; OTA revised sch 6-1-12.pdf; Appendix A TSA MOA MPA Camera policy.docx

Tom.

Here are the copies I have of the CCTV OTA/MOA documentation (originals and modifications) that exist between MASSPORT and TSA HQ. Appendix A describes MASSPORT's Camera Policy. My POC at MASSPORT for the camera system is Bill Hall – 617.568.3992.

I'm not sure if we or MASSPORT should respond to this request.

Let me know if you need anything else.

R/
Roger

From: Brady, Thomas C (TSA)
Sent: Thursday, January 02, 2014 8:01 AM
To: Blais, Roger
Subject: FW: 2013-TSFO-01096

Roger
We received a FOIA request from a passenger back in February, 2013 who is looking for the following information---

> * any contract/agreement with other agencies regarding surveillance,
> or maintenance of surveillance footage, at Logan airport

Would you have the information or know a point of contact
Thanks
Tom

From: Gearing, Paul <CTR>
Sent: Thursday, January 02, 2014 7:39 AM
To: Brady, Thomas C (TSA)
Cc: TSA.FOIAPOCResponses
Subject: 2013-TSFO-01096

Attached.

Paul Gearing
Freedom of Information Act Branch, FOIA Assistant